



Application Packaging Lore Book

Jose Schenardie

Sponsors



That's a me



Jose Schenardie

Microsoft MVP · Security

Role

CTO - Devicie

Focus

Intune · R&D · AI

Blog

<https://msendpointmgr.com>

<https://intune.tech>



Agenda

- Getting Started with App Packaging
- Packaging Process
- Public / Private Repos
- Tools





Getting Started with App Packaging

It all starts with a need



I need to install software
X for department/user Y
and keep it up to date

Followed by an evaluation of



Risk

How critical is this software and its updates and how often are they released?

How quick do I need to get updates packaged and deployed?

How likely is this software to have a vulnerability exploited in the wild?

Followed by an evaluation of



Effort

How long will it take for me to package this software:

Manually

With automation

Using a third party*

Followed by an evaluation of



*Cost

Is the cost:

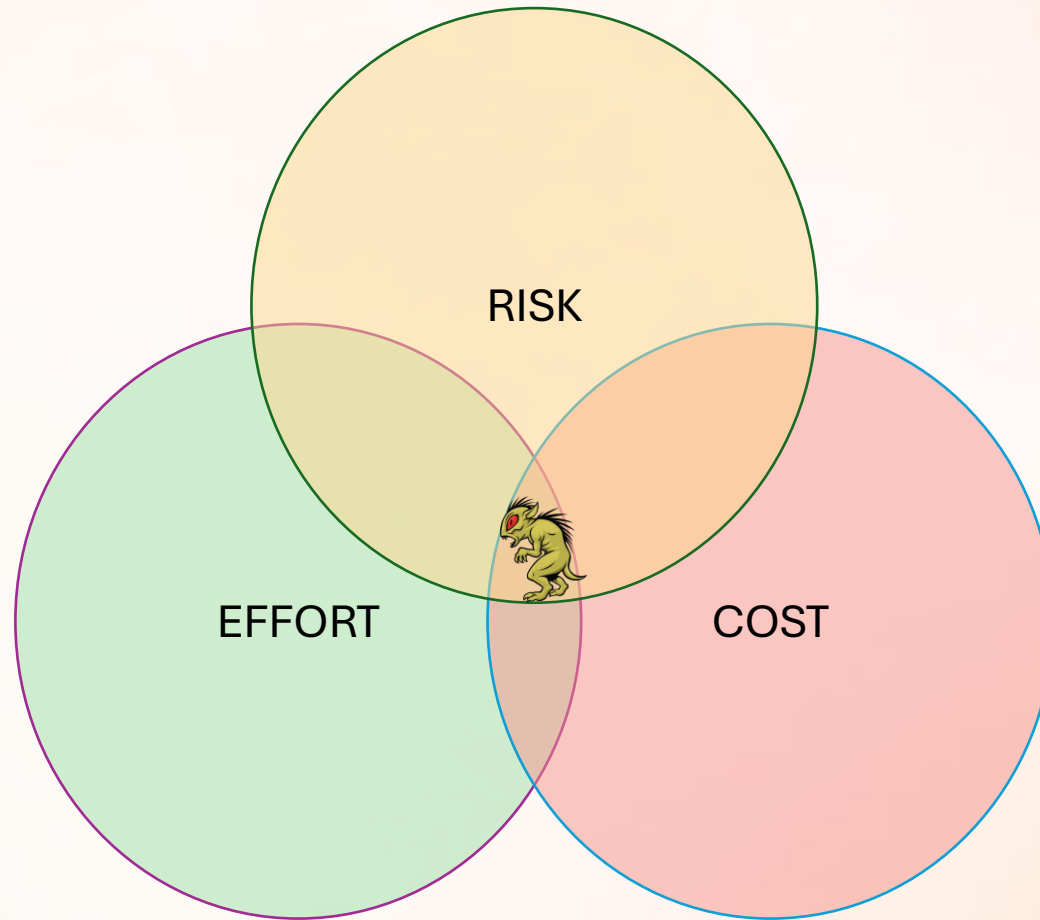
Man hours?

Per user per month?

For resources of open-source solution (deployed on my cloud)

Embedded on license (E5/E7)

That leads us to





Packaging Process

It all starts with metadata



Media file (aka MSI, EXE, ZIP, MSIX)

- Download URL
- Hash Validation

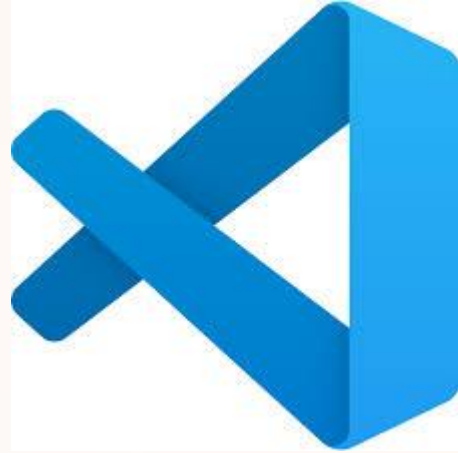
Detection information

- ARP Version (*custom)
- MSI Version
- File Version
- Registry



Example 1

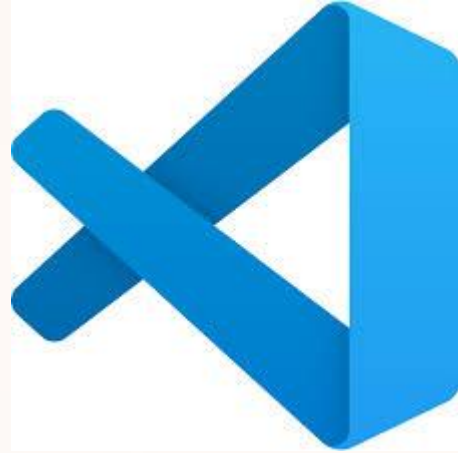
Vendor Website



<https://code.visualstudio.com/download#>

<https://code.visualstudio.com/sha/download?build=stable&os=win32-x64>

Vendor Website



<https://vscode.download.prss.microsoft.com/dbazure/download/stable/560a9dba96f961efea7b1612916f89e5d5d4d679/VSCoSetup-x64-1.116.0.exe>

Self Update Snooping (internal api)



The screenshot shows the Fiddler Classic application running in a Windows Sandbox. The window title is "Progress Telenik Fiddler Classic". The interface includes a menu bar (File, Edit, Rules, Tools, View, Help), a toolbar with various icons, and a main workspace. A yellow banner at the top of the workspace reads "Fiddler Classic downgrades HTTP/2 requests - see real behavior with [Fiddler Everywhere](#)".

The left pane displays the message: "No Sessions captured (or all were hidden by filters)".

The right pane displays the message: "Please select a single Web Session to inspect".

At the bottom of the window, a status bar shows "Capturing" and "All Processes" with a count of "0". A small tooltip at the bottom left reads "[QuickExec] ALT+Q > type HELP to learn more".

Update URLs



1.104.1 x64

<https://update.code.visualstudio.com/api/update/win32-x64/stable/0f0d87fa9e96c856c5212fc86db137ac0d783365>

1.105.0 x64

<https://update.code.visualstudio.com/api/update/win32-x64/stable/03c265b1adee71ac88f833e065f7bb956b60550a>

1.105.0 arm64

<https://update.code.visualstudio.com/api/update/win32-arm64/stable/03c265b1adee71ac88f833e065f7bb956b60550a>

Copy and paste does not work between projects opened in dev containers #271012

Open



Does this issue occur when all extensions are disabled?: Yes (except those needed for dev containers)

```
Version: 1.105.0 (Universal)
Commit: 03c265b1adee71ac88f833e065f7bb956b60550a
Date: 2025-10-08T14:09:35.891Z
Electron: 37.6.0
ElectronBuildId: 12502201
Chromium: 138.0.7204.251
Node.js: 22.19.0
V8: 13.8.258.32-electron.0
OS: Darwin arm64 25.0.0
```

Steps to Reproduce:

1. Open two different projects in a dev container (mounted source code)
2. Select a file in project A explorer, and select copy from the right click menu.
3. Switch to project B, and select paste from the right click menu in the explorer.

The following error popup will occur:

```
The file(s) to paste have been deleted or moved since you copied them. Error: ENOENT: no such file or directory, stat
```

Copy/Cut and Paste do not seem to have awareness of the dev container. Ideally, there would be clipboard metadata added that would allow VSCode to reference the host pathname, or otherwise identify that the origin of the paste operation was in another dev container, and there would be some mechanism to accomplish the paste operation.



2

vs-code-engineering added [new release](#) on Oct 13, 2025





Example 2

Vendor Website

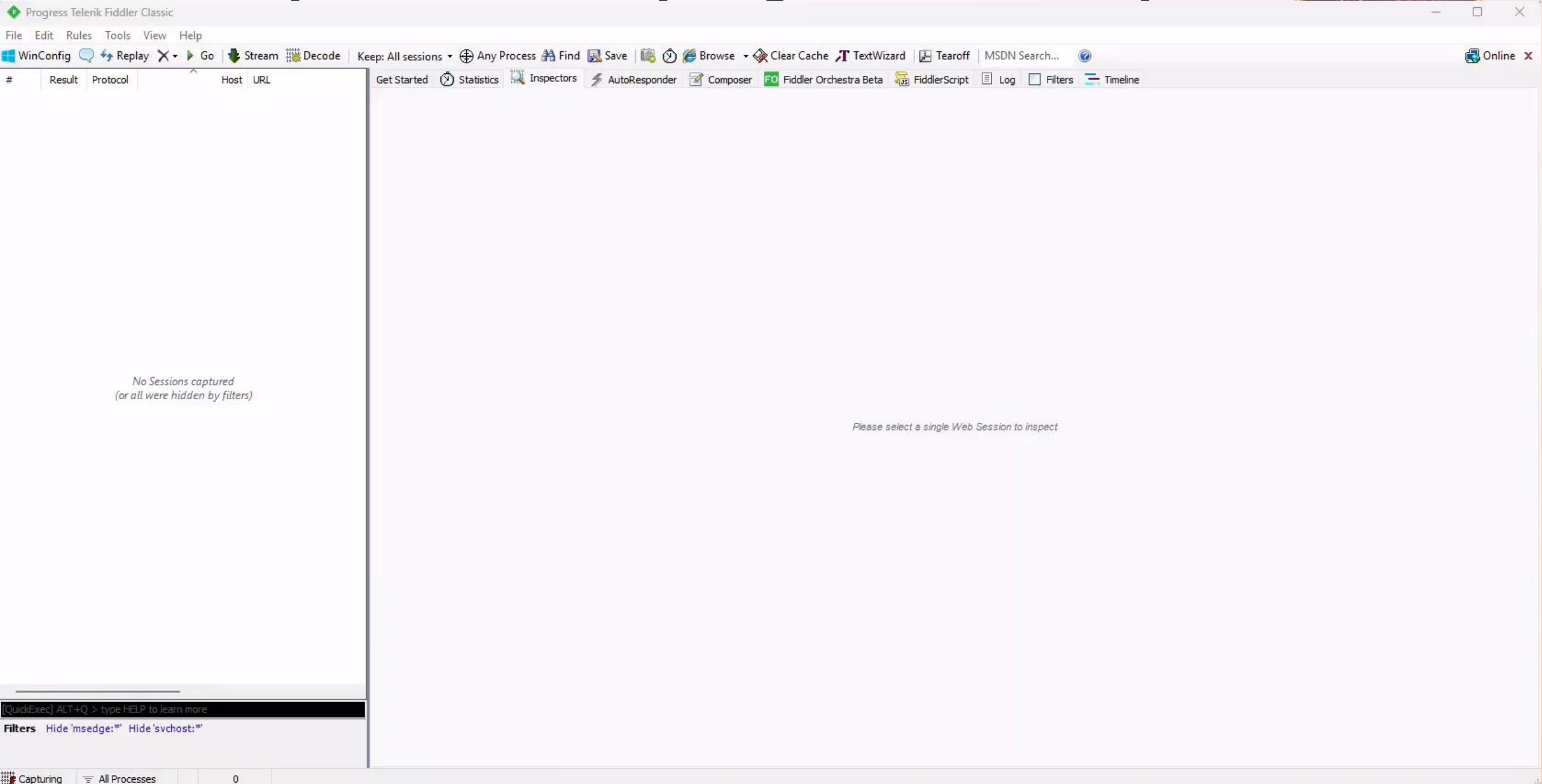


<https://notepad-plus-plus.org/downloads/>

<https://notepad-plus-plus.org/downloads/v8.9.1/>

<https://github.com/notepad-plus-plus/notepad-plus-plus/releases/download/v8.9.1/npp.8.9.1.Installer.x64.exe>

Self Update Snooping (internal api)



Malware URLs



Notepad++ Official Update Mechanism Hijacked to Deliver Malware to Select Users

Feb 02, 2026

Notepad++ Hijacked by State-Sponsored Hackers

2026-02-02

Following the security disclosure published in the v8.8.9 announcement <https://notepad-plus-plus.org/news/v889-released/>, the investigation has continued in collaboration with external experts and with the full involvement of my (now former) shared hosting provider.



the v8.8.9 announcement <https://notepad-plus-plus.org/news/v889-released/> with external experts and with the full involvement of my (now former) shared hosting provider.

MALWARE

Nation-State Actors Exploit Notepad++ Supply Chain

8 min read

...tDownloadUrl.php?version=8.9¶m=x64

<https://github.com/notepad-plus-plus>

Notepad++ Supply Chain Attack & Chrysalis Backdoor

8 MIN READ | MARCH 02, 2026

SUMMARIZE WITH:

ChatGPT

perplexity

Google AI

Between June and December 2025, the update infrastructure for the popular text editor Notepad++ was compromised, allowing threat actors to distribute malicious updates to targeted users. The breach originated from an incident at the hosting provider level, which granted the attackers access to internal services for several months.

During this period, three distinct infection chains were observed, targeting organizations in the government, financial, and IT sectors across Vietnam, El Salvador, Australia, and the Philippines [1].

id/v8.9

Notepad++ Hijacked by State-Sponsored Hackers

2026-02-02

Following the security disclosure published in the v8.8.9 announcement <https://notepad-plus-plus.org/news/v889-released/>, the investigation has continued in collaboration with external experts and with the full involvement of my (now former) shared hosting provider.

According to the analysis provided by the security experts, the attack involved infrastructure-level compromise that allowed malicious actors to intercept and redirect update traffic destined for notepad-plus-plus.org. The exact technical mechanism remains under investigation, though the compromise occurred at the hosting provider level rather than through vulnerabilities in Notepad++ code itself. Traffic from certain targeted users was selectively redirected to attacker-controlled malicious update manifests.

The incident began in June 2025. Multiple independent security researchers have assessed that the threat actor is likely a Chinese state-sponsored group, which would explain the highly selective targeting observed during the campaign.

An incident-response (IR) plan was proposed by the security expert, and I facilitated direct communication between the hosting provider and the IR team. After the IR team engaged with the provider and reviewed the situation, I received the following detailed statement from the provider:



This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<GUP>
  <NeedToBeUpdated>yes</NeedToBeUpdated>
  <Version>8.9.3</Version>
  <Location>https://1.76.155.202/update/update.exe</Location>
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
      <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
      <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
      <Reference URI="">
        <Transforms>
          <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#sha256"/>
        <DigestValue>H/yYUXFpLXDG6atF3sz8f6AydwywFRswQkWkuBnxCSQ</DigestValue>
      </Reference>
    </SignedInfo>
    <SignatureValue>WmMitCHgdszw+R8aOvN2o0X/aOE/BHmGauv+LECKUBuk9XMRYjR1r0ZYdTU9NdZcYHhXhQacHBzey7azhfOnWVGg6b3MDvy5TWEfEEDcK5yW5HP/Bv7eW004jf70Wr6ndDs5cHUEa+FTP+opdR5ZLe6QX70YJX4JfcX8n7oDfznDVag8dx8u18bHAKw/+wP
    </SignatureValue>
  </Signature>
  <KeyInfo>
    <X509Data>
      <X509Certificate>MIIHKDCCBRCgAwIBAgIMBfDY9am8ARXwiCZMA0GCSqGSIb3DQEBCwUAMFkxCzAJBgNVBAYTAKJFMFRkFwYDVQQKEExBHBG9iYWxTaWduIG52LXNhMS8wLQYDVQQDEyZHBG9iYWxTaWduIEEdDQyBSNDUgQ29kZVNPZ2Z5pbmcgQ0EgMjAyMDAeFw0yNT
    </X509Data>
  </KeyInfo>
</Signature>
</GUP>
```

GitHub Version Control



<https://api.github.com/repos/{vendor}/{project}/releases/latest>

```
<Location>https://github.com/notepad-plus-plus/notepad-plus-plus/releases/download/v8.9.1/npp.8.9.1.Installer.x64.exe</Location>
```

<https://api.github.com/repos/notepad-plus-plus/notepad-plus-plus/releases/latest>

<https://github.com/notepad-plus-plus/notepad-plus-plus/releases/latest>

GitHub Version Control



```
← ↻ 🏠 🔒 https://api.github.com/repos/notepad-plus-plus/notepad-plus-plus/releases/latest
Pretty-print 
},
"node_id": "RE_kwDDAaffEG84RGRLO",
"tag_name": "v8.9.2",
"target_commitish": "master",
"name": "Notepad++ release 8.9.2",
"draft": false,
"immutable": false,
"prerelease": false,
"created_at": "2026-02-16T13:24:19Z",
"updated_at": "2026-02-16T13:31:10Z",
"published_at": "2026-02-16T13:27:08Z",
"assets": [
```



Example 3

Vendor External API



<https://support.logi.com/hc/en-au/articles/360025297893-Logitech-Options>

Vendor External API

https://support.logi.com/hc/en-au/articles/360025297893-Logitech-Options

InPrivate browsing

InPrivate search with Microsoft Bing

✔ What InPrivate browsing does

- Deletes your browsing info when you close all InPrivate windows
- Saves collections, favorites, and downloads (but not download history)
- Prevents Microsoft Bing searches from being associated with you

✘ What InPrivate browsing doesn't do

- Hide your browsing from your school, employer, or internet service provider
- Give you additional protection from tracking by default
- Add additional protection to what's available in normal browsing

Always use "Strict" tracking prevention when browsing InPrivate

If this is off, we'll use the same tracking prevention setting as a normal browsing window

Cookies aren't shared during InPrivate

InPrivate browsing keeps cookies private to help prevent sites from sharing your data across the web. If a site doesn't work, you can temporarily allow cookie access.

[More details](#)

Network tab in browser developer tools

Name	Status	Type	Initiator	Size	Time	Fulfilled by
No search results						

Type and press Enter to search

Currently recording network activity

Perform a request or refresh the page by using the "Reload page" button or by pressing Ctrl + R. [Learn more](#)

[Reload page](#)

Vanity URLs



<https://zoom.us/client/latest/ZoomInstaller.exe?archType=winarm64>

<https://code.visualstudio.com/sha/download?build=stable&os=win32-arm64>

Vanity URLs



Cause issues with:

- Gradual Rollouts
- SHA verifications



Public / Private Repos

Definition



- Private repo
<https://apps.microsoft.com/home>
- Public repo
<https://github.com/microsoft/winget-pkgs>
- Enterprise Application Manager repo =
*****.com



Private Repo Getting Started



Create account (MS Account)

Validate ID / Company

Account setup

App submission

App certification

Private repo Account Type



Microsoft Store Developer Platform



Individual developer

For hobbyists, students, and individual developers publishing under their own name.

Free



Company account

For businesses, freelancers, and teams publishing under a company or organization name.

\$99 one-time fee

Private repo ID Verification



Ready to verify your identity

To complete verification, you'll need to:

- Take a live photo of your government-issued photo ID and selfie
- Ensure the ID is non-expired and all text is clearly readable
- Present the original physical document (not scanned copy)

[Begin verification process](#)

Your ID information is used solely for verification and processed securely per Microsoft's privacy standards.

Private repo ID Verification



Switch to mobile to continue

Scan this code directly using your phone's camera. If that doesn't work, try a QR scanning app.

Scan Me



Private repo ID Verification




ID verification complete!

Your ID has been verified.
You can now continue to the next step.

Private repo Account Setup






Getting everything ready...


We're preparing your publisher environment before starting account creation.

Progress 0%

Preparing your account...

Private repo Account Setup



 **Account setup complete!**

Your developer account is ready.
Start building and managing your apps in Partner Center.

[Go to Partner Center dashboard](#)

App Submission



- Choose app type
 - MSIX or PWA
 - EXE or MSI
 - Game
- Reserve Name
- Pricing and Availability (worldwide or specific countries)
- Properties (Category, support, etc)
- Age Ratings
- Packages (Windows versions)
- Store listings (extra languages)
- Submission Options (ASAP, date, manual)

App Certification



- **Security tests:** This first test checks your app's packages for viruses and malware. If your app fails this test, you'll need to check your development system by running the latest antivirus software, then rebuild your app's package on a clean system.
- **Technical compliance tests:** Technical compliance is tested by the Windows App Certification Kit.
- **Content compliance:** The amount of time this takes varies depending on how complex your app is, how much visual content it has, and how many apps have been submitted recently. Be sure to provide any info that testers should be aware of in the Notes for certification page.

*Between 1-3 business days

[The app certification process for MSIX app](#)

Welcome to MS Store



Microsoft Store Home Apps Games About

Search: 7-zip Multi-app install

Results for "7-zip"

Filters

- All departments
- Apps
- Games
- Devices
- Memberships

BreeZip: RAR & ZIP

4.7 ★ | Apps | Productivity | Free

BreeZip is a tool to "unarchive" many different kinds of archive files - an alternative to winrar, winzip & 7zip on Windows 10 & Windows...

AukZip - RAR Zip

4.7 ★ | Apps | Utilities & tools | Free

AukZip is a superior utility for viewing, extracting archives, and compressing files into archives. An alternative to winrar, winzip, 7z...

Cool File Viewer - open rar, docx and more

4.5 ★ | Apps | Productivity | Free

Cool File Viewer allows you to view any file on your PC. Simply select any file via the program window without first having to...

Zip Unzip - rar,&7z compression

4.8 ★ | Apps | Utilities & tools | Free

A powerful utility for handling RAR, ZIP, and 7z archives with ease. ★★★★★ "Opens everything fast—super easy to use. A solid 5...

ZIP RAR Rar Zip Extractor Pro

4.1 ★ | Apps | Utilities & tools | Free

Use Rar Zip Extractor Pro for packing and unpacking files without any difficulties! Rar Zip Extractor Pro supports all popular formats...

Files App

4.0 ★ | Apps | Productivity | \$9.99

Files is an open-source modern file manager for Windows, featuring tabs, columns, and dual-pane support for seamless multitasking...

8 Zip - unpack RAR, ZIP, 7z

4.1 ★ | Apps | Utilities & tools | Free

Out with the old, in with the new. The powerful archiver 8 Zip has expanded its set of capabilities with the new Continuum, Cortana...

Zip Extractor And Unzip Pro

4.6 ★ | Apps | Utilities & tools | Free

Zip Extractor Pro is a file archiver utility. The application provides an unified, natively portable, cross-platform file manager and archive...

Zip Rar Extractor Store Edition

4.1 ★ | Apps | Productivity | Free

Zip Rar Extractor Store Edition is the fastest and the simplest archiver. Our application is built using .NET technology, ensuring a...

Total File Commander Pro

3.9 ★ | Apps | Utilities & tools | Free

Total File Commander Pro is the ultimate solution for efficiently managing and organizing your files on Windows. With its powerful...

File Viewer Plus

4.7 ★ | Apps | Utilities & tools | Free

File Viewer Plus 6 is now available — and it's packed with new features! Organize your files with the all-new file manager, Conver...

Cloud Drive for Storage Service

3.6 ★ | Apps | Entertainment | Free

Introducing Cloud Drive - Your Ultimate File Management Solution for Windows Devices Discover the power of seamless fi...

File Viewer Max

4.5 ★ | Apps | Utilities & tools | Free

Looking for a way to open your files? Try File Viewer Max. File Viewer Max supports over 500 file formats across six popular categories...

Total Zip: Rar, Zip and 7Z Extractor

4.6 ★ | Apps | Utilities & tools | Free

Total Zip is a powerful archive management tool designed to help you manage and extract archive files on the Windows platform...

Unzip Expert

4.8 ★ | Apps | Utilities & tools | Free

Unzip is a management tool that focuses on quickly decompressing and compressing files! This is a very fast and very easy to use zip fi...

Public Repo Getting Started



Create account (Github Account)

~~Validate ID / Company~~

~~Account setup~~

App submission


App certification

Account Setup

Github Signup

Sign up for GitHub

 Continue with Google

 Continue with Apple

or

Email*

Email

Password*

Password

Password should be at least 15 characters OR at least 8 characters including a number and a lowercase letter.

Username*

Username

Username may only contain alphanumeric characters or single hyphens, and cannot begin or end with a hyphen.

Your Country/Region*

Australia

For compliance reasons, we're required to collect country information to send you occasional updates and announcements.

Email preferences

Receive occasional product updates and announcements

Create account >

By creating an account, you agree to the [Terms of Service](#). For more information about GitHub's privacy practices, see the [GitHub Privacy Statement](#). We'll occasionally send you account-related emails.



App Submission



Wingetcreate

wingetcreate new url

Komac

komac token add

komac new

App Certification

Pipelines - Runs for WinGetSvc-Validation



Control	What it does?	Why It Really Matters?
PR-only, hardened pipeline	Validation runs only on pull requests , with no secrets exposed to forks	Stops attackers from abusing the pipeline itself to steal tokens or run arbitrary code
Manifest + policy enforcement	Every submission must strictly follow WinGet schemas and policies	Prevents deceptive packages, typosquatting, and metadata trickery
Installer hash verification (SHA256)	The installer's hash must match what's declared in the manifest	Blocks silent binary swaps, CDN compromise, and post-submission tampering
Malware scanning + SmartScreen reputation checks	Installers are scanned and Microsoft reputation data is consulted before approval	Catches known malware before it ever reaches users and flags low-trust, newly weaponized, or suspicious installers
Sandbox install & uninstall testing	Package is installed and removed in an isolated environment	Detects fake silent installs, persistence tricks, and broken installers
Manual review as backstop	Validate all new packages and checks other suspicious things	Final human component to verify things machines can't (I hope 😊)

App Certification

Pipelines - Runs for WinGetSvc-Publish



Control	Why It Really Matters?
Malicious PR publishes package	Publish pipeline cannot run from PRs
Fork contributor steals secrets	No secrets exposed to forks
Tampering between validation and publish	Git commit immutability + full history
Publishing unreviewed binaries	No binaries are built or uploaded
Silent feed mutation	Azure RBAC + storage auditing
Replay / partial publish	Batch mode + single authoritative feed

App Certification



[winget-pkgs/Tools/ManualValidation at master · microsoft/winget-pkgs](#)

[New version: BenthicSoftware.GoldSqall.2 version 2.4.0.240 by schenardie · Pull Request #349203 · microsoft/winget-pkgs](#)

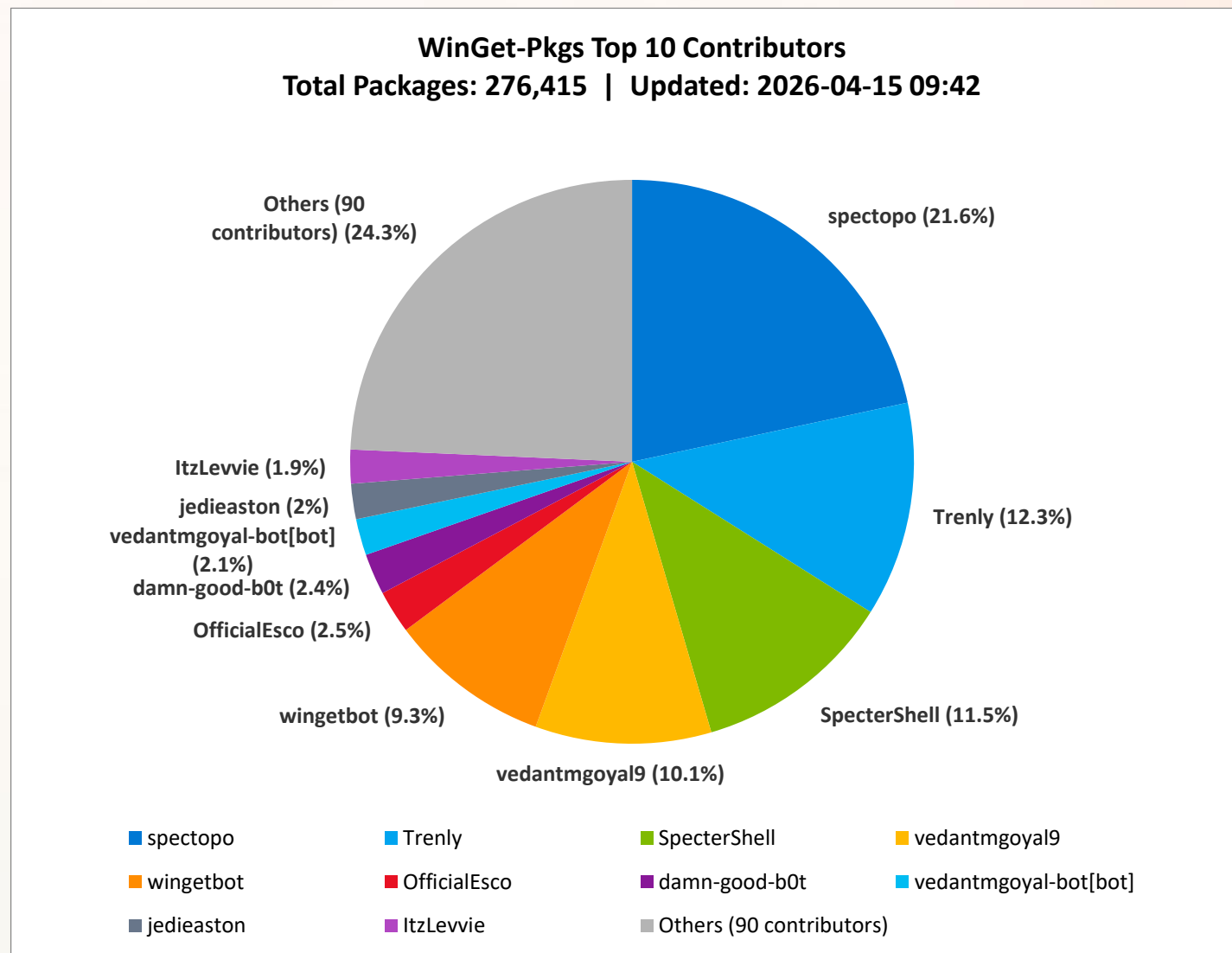
wingetbot commented last month Collaborator ⋮

Inconsistencies detected in package `BenthicSoftware.GoldSqall.2` version `2.4.0.240` based on published version `2.2.0.222`

- Missing property `ReleaseNotes`
- Missing property `ReleaseNotesUrl`

😊

Submission Statistics



[source](#)



Tools

Testing Apps



[Run in Sandbox - Joly0](#)

[Intunewin RightClick Extract - Damien Van Robaeys](#)

[PsExec - Sysinternals | Microsoft Learn](#)

Re-packaging Apps



[Master Packager](#)

[InstEd It! - Download instead](#)

[PSAppDeployToolkit](#)

Paas Packaging



[Intune App Factory - MSEndpointMgr](#)

SaaS Packaging



[IntuneGet | Free Intune App Deployment Tool](#)

Intune Awesome Packaging



Awesome Intune - Browse Packaging Solutions

- IntuneWin Utility** Packaging
IntuneWin Utility is a modern GUI tool for creating Microsoft...
Mohammed O... 2.1k ↑ View
- WinGet-PSADT-GUI-Tool** Packaging
WinGet-PSADT-GUI-Tool is a Windows PowerShell WPF GUI that...
Dhiraj Dhote 2k ↑ 1 View
- IntuneGet** Packaging
A web-based tool that automates deploying Windows...
Ugur Koc 3.4k ↑ 1 View
- PSADT Helper** Packaging
PSADT Helper has the function in it, it lets you easily migrate thos...
Roman Padrun 3.1k ↑ 1 View
- IntuneWinAppUtil GUI** Packaging
IntuneWinAppUtil GUI is a PowerShell-based WPF wrapper for...
Giovanni Solone 3.4k ↑ 2 View
- PSADT Script Generator** Packaging
Automatically generate PSADT deployment scripts for new...
Robert L 1.8k ↑ 1 View
- PSAppDeployToolkit** Packaging
PSAppDeployToolkit is a PowerShell-based, open-source...
PSAppDeployT... 6.9k ↑ 4 View
- swiftDialog ESP Configurator** Packaging
Built for MacAdmins who want smooth deployments with great...
Artem Brening 6k ↑ 3 View

- Wintuner** Packaging
WinTuner is a tool that lets you take any WinGet app and upload ...
Stephan van R... 4k ↑ 4 View
- IntuneAppDoc.com** Packaging
IntuneAppDoc.com automates creation of comprehensive...
Morten Glimme 1.9k ↑ 1 View
- IntuneBrew** Packaging
A macOS app deployment and patch management solution for...
Ugur Koc 3.7k ↑ View
- Intune-App-Sandbox** Packaging
Intune-App-Sandbox is a testing utility for PowerShell-based...
Maciej Horbacz 3.4k ↑ 1 View
- AutomaTuner** Packaging
A Python tool that automates packaging and deploying...
Ayoub Sekoum 18.7k ↑ 2 View
- Deployment Editor** Packaging
A visual software packaging editor for creating Windows...
Tugay Taskin 11k ↑ 2 View
- IntunePrepTool** Packaging
A PowerShell GUI tool for streamlining application packaging for...
Rink Turksma 2.8k ↑ View
- IntuneWin32App** Packaging
A PowerShell module for managing the complete lifecycle of...
Nickolaj Anders... 2.6k ↑ View

Please rate this session on
Sched.com

We would love to hear what
you liked and how we could
improve!



Thanks!